Archer Supply Chain Security

Overview

Archer's supply chain security aims to manage risk via a layered approach which protects the assets and infrastructures involved in the production of its products. This begins with our internal network environment and associated assets which are secured through controls such as strong password enforcement, virus detection, email attachment scanning, system and application patch compliance, intrusion detection, and firewalls. Additional controls have been implemented to protect against malware and misuse of assets.

The principles of "least privilege" and "separation of duties" guide key controls throughout the supply chain to help prevent misuse of data access across the business. These principles ensure that access to sensitive information is only granted to individuals, as needed, to perform assigned duties. In addition, employees maintain a culture of security guided by annual security awareness and compliance training designed to mitigate risky behaviors that may put products at risk throughout the supply chain.

DevOps Supply Chain

Software engineering teams apply best practices to integrate security throughout the DevOps process. A robust cybersecurity program improves software integrity by preventing unauthorized access to source code, minimizing the potential for malware to be introduced into a product before it is released to a customer and monitoring it after release.

Sourcing

Archer has a comprehensive open source software process. Open source code included in our software products must be documented and approved by appropriate internal engineering and legal leadership personnel.

Source code is peer reviewed on each commit, and engineers are instructed to ensure code adheres to security best practices. Additionally, software engineering teams perform design analysis activities such as threat modeling, static code analysis, and scanning and security testing intended to discover and address security defects throughout the development lifecycle. Such prescriptive controls are intended to ensure that development teams code defensively to prevent specific prevalent security issues including those found in the OWASP Top 10 or SANS Top 25.

Delivery

Pipelines

Systems are built in accordance with industry best practices with minimal access granted. Systems are appropriately hardened, reviewed on a regular basis, and undergo regular security checks and updates. Unnecessary services are disabled, and each host is monitored and updated in accordance with change control procedures via an update manager.

As an additional check to verify that Archer has properly secured its systems, third-party penetration tests are conducted against both applications and infrastructure by skilled/trained personnel working for organizations under contract to Archer.

Continuous Monitoring

Archer performs continuous real-time security monitoring of its infrastructure by way of a SIEM. A security operations team runs infrastructure scans regularly, and high priority items are flagged for prompt remediation.

Downloads

Code released for customer download is processed through our Code Signing Process which includes code signing and verification, publish of checksums for customer verification, and where appropriate, third-party DLL signing. Each step includes an internal test check.

Continuous Patch Releases (CPRs)

Because new vulnerabilities are discovered regularly across the industry, Archer's security program does not end at code release. A product security incident response process is responsible for coordinating the response and disclosure of identified product vulnerabilities. Vulnerabilities are addressed in monthly CPRs and applied to infrastructure environments on a regular cadence. CPRs are cumulative and released monthly for customers to download and install in their own environments, as well. Security advisories are issued with a goal to provide customers timely information about newly identified vulnerabilities and ways to mitigate their impact.